Montana Operations Manual ***Standard***	**Policy Number**	1240.XS1
	Effective Date	July 1, 2012
	Last Revised	August 16, 2011
Issuing Authority	State of Montana Chief Information Officer	

Information Security Access Control

I. Purpose

This Information Security Access Control Standard establishes the specifications and process requirements to implement the access security controls specified within the National Institute of Standards and Technology Special Publication 800-53 (NIST SP800-53) Recommended Security Controls for Federal Information Systems and Organizations (NIST SP800-53). Implementation of these NIST controls is required by the Statewide Standard: Information Security Programs.

II. Scope

This standard applies to all executive branch Agencies, excluding the university system.

III. Statement of Standard

The requirements and specifications for this Standard are derived from the National Institute of Standards and Technology Special Publication 800-53 (NIST SP800-53) Recommended Security Controls for Federal Information Systems and Organizations (NIST SP800-53), Federal Information Processing Standard publications (FIPS PUB), and other NIST publications as specifically referenced herein.

A. Management Requirements

Each Agency shall ensure that an organization structure is in place to:

1. assign information security responsibilities;

2. perform Access Control for Information Systems;

3. allocate adequate resources to implement Access Controls;

4. develop processes and procedures to measure compliance with this Standard; and

5. establish and evaluate performance measures to assess implementation of this Standard and subordinate procedures.

a. Department Heads
The department head (or equivalent officer) has overall responsibility for providing adequate resources to support the protection of information system(s) and communication.

b. Information Security Officer
The Information Security Officer (also known as the Information Systems Security Officer) may be the same individual designated by the department or head to administer the Agency's security program for data under 2-15-114, MCA, Security Responsibilities of Departments for Data. Specific responsibilities under this Standard are:

(a) evaluate Access Control issues within the department and all component organizations;

(b) provide resolution recommendations to the department head and division administrators, if any; and

(c) develop Agency policies, standards, and procedures as required.

B. Performance Requirements

Each Agency shall develop and implement Access Controls based on an evaluation of Information Systems, derived from the NIST *risk management framework,* which:

1. uses the categorization standards of:

a. Federal Information Processing Standards Publication (FIPS PUB) 199 Standards for Security Categorization of Federal Information and Information Systems

b. Federal Information Processing Standards Publication (FIPS PUB) 200 Minimum Security Requirements for Federal Information and Information Systems;

2. uses the Access Controls stipulated within NIST SP800-53 Recommended Security Controls for Federal Information Systems and Organizations;

3. specifies levels of Access Controls based upon the following requirements:

a. As determined by completion of the risk management process specified in and based upon NIST SP800-39 Managing Information Security Risk – Organization, Mission, and Information System View. After review of the risk assessment(s), the department or Agency management shall determine any changes in the level of process, standards and controls. or,

b. Implements the low – impact baseline control set defined within NIST SP800-53 Recommended Security Controls for Federal Information Systems, Low-Impact Baseline Contingency Planning family (Annex 1);

2. implements this Standard through procedure(s);

3. reviews Access Controls and processes and procedures as required, and implements authorized changes to policy, standard(s), or procedure(s); and

4. is based upon the latest publicly available versions of publications referenced within this Standard *at the date of approval* of this Standard. (Note: Because newer versions of the publications referenced herein become available from time-to-time, each Agency is encouraged to stay current by using the most recent versions, as deemed feasible by each Agency. Future revisions of this Standard will reference then currently-available versions.)

IV. Definitions

Agency: Any entity of the executive branch, excluding the university system. Reference 2-17-506(8), MCA.

Information Resources: Information and related resources, such as personnel, equipment, funds, and Information Technology. Reference 44 U.S.C. Sec. 3502.

Information Security: The protection of information and Information Systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Reference 44 U.S.C. Sec. 3542.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Reference 44 U.S.C. Sec. 3502.

Information Technology: Hardware, software, and associated services and infrastructure used to store or transmit information in any form, including voice, video, and electronic data. Reference 2-17-506(7), MCA.

Refer to the National Information Assurance (IA) Glossary for common Information Systems security related definitions.

Refer to the NIST SP800-53 Recommended Security Controls for Federal Information Systems and Organizations. Appendix B Glossary for security control definitions.

Refer to the Statewide Information System Policies and Standards Glossary for a list of local definitions.

VI. Changes and Exceptions

The Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards governs standards changes or exceptions. Submit requests for a review or change to this instrument by Action Request form. Submit requests for exceptions by an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

VII. Closing

Direct questions or comments about this Standard to the State of Montana Chief Information Officer at SITSD Service Desk (at http://servicedesk.mt.gov/ess.do), or:
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

VIII.References

A. Legislation

1. 2-15-112, MCA – Duties and powers of department heads

2. 2-15-114, MCA – Security responsibilities of departments for data.

3. 2-17-534, MCA – Security responsibilities of department.

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

1. Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards

2. Statewide Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

C. Standards, Guidelines

1. Guide To NIST Information Security Documents

2. ITL Bulletin - Guide for Developing Security Plans for Information Technology Systems

3. NIST SP800-18 Guide for Developing Security Plans for Federal Information Systems

4. NIST SP800-39 Managing Information Security Risk – Organization, Mission, and Information System View

5. ITL Bulletin: Integrating IT Security into the Capital Planning and Investment Control Process

6. NIST SP800-53 Recommended Security Controls for Federal Information Systems and Organizations

7. NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 1, Low-Impact Baseline Access Control (AC) family

8. NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 2, Moderate-Impact Baseline Access Control (AC) family

9. NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 3, High-Impact Baseline Access Control (AC) family

10. Federal Information Processing Standards Publication (FIPS PUB) 199 Standards for Security Categorization of Federal Information and Information Systems

11. Federal Information Processing Standards Publication (FIPS PUB) 200 Minimum Security Requirements for Federal Information and Information Systems

IX. Administrative Use

Scheduled Review Date: January 1, 2012

Changes: NA